Computing Security
Secure systems, secure data, secure people, secure business

Top 3 data security threats

Roman Foeckl, CEO and founder of CoSoSys, offers his insights on how to mitigate threats through a sound data security plan

Sometimes we feel like we keep repeating ourselves and then we realise that's our job as vendors: to speak about the potential threats to data security with every opportunity we get and hope that CSOs are one step closer to mitigating threats by implementing a sound data security plan.

Today, we want to emphasise three of the most pre-eminent threats:

1. Cloud storage applications
We see a lot of companies that use apps like Dropbox, Google Drive etc, which fall under what's called grey IT or a grey area, because IT security people know they are being used, but there are no clear restrictions or permissions. At most, they have a regulation stating that employees are not allowed to share confidential data with third parties; but where to share it or what qualifies as a third party is not mentioned. Moreover, the regulation is usually a piece of paper in a pile of documents that employees sign and then forget about.

Businesses need to create more 'live' procedures after studying the cloud compliance issues that arise from the use of cloud storage. Where will the data be kept, what data can be saved on the cloud and what should be kept in-house, how secure is the cloud storage platform? These are some of the questions to be answered, in order to know the next steps for a clear objective regarding data security.

IT security staff should also consider cloud encryption solutions. They should make sure that all stored information is secured in an encrypted container, for which they hold and manage the encryption key. Additionally, they should use Data Loss Prevention (DLP) solutions to restrict file sharing according to the content of the document - e.g, block transfers of documents containing Credit Card Numbers (CCNs).

2. Mobile devices
Mobility is a challenge for organisations. Tablets and smartphones are auxiliary devices and, in some cases, the main items for work. This translates into high volumes of corporate data residing on mobile devices. The threat emerges from the lack of consistent rules to establish what mobile device has access to what data, and in what circumstances. Context is important to set up relevant security policies for mobile devices, especially because they are carried around everywhere. With geofencing, one of the most recent innovations in Mobile Device Management (MDM), IT administrators can create security policies based on location. The camera can be blocked while the employee is at work, but allowed when at home.

There is no point denying the use of a camera in employees' spare time, away from company secrets. This is just an example, but context is becoming more and more important in mobile security, since mobile devices are an extension of computers, and there is a thin line between personal and corporate data. There needs to be a balance between restrictions and permissions, since the whole purpose of mobility is to enable workers to be more productive.

3. Insiders with or without malicious intentions
In a recent survey we conducted on our customers*, we discovered that 35% of enterprise employees think that data security is not their responsibility, while 59% think that losing a mobile device or laptop with company data doesn't represent too much of a threat. These numbers are worrying, since companies' data security depends significantly on employees' adherence to internal rules.

Organisations must create comprehensive policies and include their employees in continuous IT security education programs. With disgruntled employees, it is another story, but in both cases DLP solutions play an essential role to avoid data breaches and data thefts.
* **http://www.endpointprotector.com/resources/infographics**